REMARKS

Claim 8 has been amended to be dependent from independent claim 7, as suggested by the Examiner.

Claims 1-12 are in the case. Claims 1-3 and 5-10 stand rejected, while claims 4, 11 and 12 have been found allowable. While applicants appreciate the Examiner's allowance of claims 4, 11 and 12, it is respectfully submitted that claims 1-3 and 5-10 should also be allowed.

Claim 1-3 and 5-10 stand rejected under 35 USC 103 over admitted prior art (referred to as Admission) in view of Ferrant, US Patent Number 6,421,799. It is respectfully submitted that even if these disclosures were combined as suggested by the Examiner, the resulting method does not anticipate applicants' claims 1-3 and 5-10.

Claim 1 is set out in full:

1. A method of testing a device comprising:
providing a first data string;
providing a second data string in a memory structure;
encrypting the first data string using an encryption algorithm, to provide an encrypted data string; and
comparing a characteristic of the encrypted data string with a characteristic of the second data string.

The Examiner cites Ferrant at column 1, lines 8-33, set out in full:

> A way of testing the proper manufacturing of a ROM consists of reading its content and checking that all the stored information is correct. This test operation is lengthy and expensive, and an embarked testing device is included in a ROM. Such a device is designed for, during a test phase, successively receiving all the data stored in the memory, adding them, multiplying them, etc. according to an adequate encryption algorithm, and comparing the final result with the result expected from the memory data. When the results are equal, the memory is assumed to be good.

Thus, in Ferrant, the procedure is that all the data stored in a memory is received, and is acted on according to an encryption algorithm. This apparently corresponds to the first data string of claim 1, which is encrypted using an encryption algorithm. In Ferrant, this encrypted data string is compared with "the result expected from the memory data". In applicants' claim 1, the comparison is between the encrypted data string and the second data string <u>which is in a memory structure</u>. There is no disclosure in Ferrant that the "second data string" is in a memory structure as called for in claim 1. Rather, Ferrant only talks of an <u>expected result</u> based on memory data.

It is therefore respectfully submitted that even if the Admission were combined with the disclosure of Ferrant, the resulting method would not anticipate applicants' claim 1.

Claim 2, dependent from claim 1, is initially respectfully submitted to be allowable on the basis of this dependency. Claim 2 is also submitted to be allowable on the basis that no combination of the Admission and Ferrant would anticipate applicants' claim 2. Claim 2 calls for comparing a characteristic of the encrypted data string with a characteristic of the second data string to comprise comparing the bit length of the encrypted data string with the bit length of the second data string. The Examiner states:

> **<u>As per dependent claims 2-3 and 8-10, the combination of Admission and Ferrant discloses a</u> method as applied to claims above. Furthermore, Admission discloses the method wherein, the step of comparing a characteristic of the encrypted data string with a characteristic of the second data string comprises comparing the bit length of the encrypted data string with the bit length of the second data string. [page 1, line 16, page 6, lines 14-19]** ("*While it would be of course desirable to test the encryption function of the DUT for proper operation thereof, i.e., that the encrypted packet data string is as expected, the* **matching of resulting encrypted packet data segment against each of the possible encrypted forms is impractical**, because of the *very large number of possible encrypted forms. Therefore, what is needed is a method for testing the encryption function of a device, which method is simple and effective in use." And on page 1, lines 16 of the applicant's specification discloses that the properties of the data* ***packets includes packet length)***

Contrary to the Examiner's statement, and in accordance with applicants' specification quoted by the Examiner above, such an approach is <u>not</u> untaken because it is impractical. This is the very problem that applicants wish to overcome. While packet length is a characteristic property of a data string, the Admission method does not test for this. Claim 2 is thus respectfully submitted to be allowable on this basis also.

Claim 3, dependent from claim 2, is initially respectfully submitted to be allowable on the basis of this dependency. Claim 3 describes comparing of an initialization vector associated with the encrypted data string with an initialization vector applied in encrypting the first data string, if a match is found between the bit length of the encrypted data string and the bit length of the second data string in the memory structure. The Examiner submits that his comments with regard to claim 2 apply with equal force against claim 3. However, similar to the above analysis, while initialization vectors are involved in the Admission description, no comparison thereof as called for in claim 3 is disclosed or suggested in a combination of the Admission and Ferrant. Claim 3 is thus respectfully submitted to be allowable on this basis also.

Claim 5, dependent from claim 1, is initially respectfully submitted to allowable on the basis of this dependency. Claim 5 calls for the data string in the memory structure to be an unencrypted data string. The Examiner submits that

> **the method wherein, the data string in the memory structure is an unencrypted data string.** [*See figure 1, ref. "P1S1" and figure 2, ref. "P1S2"*]

Thus, claim 5, in conjunction with claim 1 from which it is dependent, calls for comparing a characteristic of an encrypted data string with a characteristic of an unencrypted (second) data string in the memory structure. Nowhere is such comparison disclosed or suggested in the Admission, or in any combination of the Admission and Ferrant. Indeed, applicants' specification states at page 6, lines 14-17:

> While it would be of course desirable to test the encryption function of the DUT for proper operation thereof, i.e., that the encrypted packet data string is as expected, the matching of resulting encrypted packet data segment against each of the possible encrypted forms is impractical, because of the very large number of possible encrypted forms.

Claim 5 is thus respectfully submitted to be allowable on this basis also.

Independent claim 6 includes limitations similar to those set forth in claims 1 and 3, and thus the arguments set forth in favor of the allowability of claim 1 and 3 apply with equal force in favor of claim 6.

Independent claim 7 also includes limitations similar to those set forth in claims 1 and 3, and thus the arguments set forth in favor of the allowability of claims 1 and 3 apply with equal force in favor of claim 7.

Claim 8, dependent from claim 7, is initially respectfully submitted to be allowable on the basis of this dependency. Claim 8 includes limitations similar to those set forth in claim 2, and thus the arguments set forth in favor of the allowability of claim 2 on its own merit apply with equal force in favor of claim 8.

Claim 9, dependent from claim 8, is initially respectfully submitted to be allowable on the basis of this dependency. In accordance with claim 9, if a match is not found between the bit length of the encrypted data string and the bit length of a data string in the memory structure, a comparison step is undertaken comparing the bit length of the encrypted data sting with the bit length of another data string in the memory structure. Nowhere is such approach disclosed or suggested in any combination of the Admission and Ferrant. Claim 9 is thus respectfully submitted to be allowable on this basis also.

Claim 10, dependent from claim 8 is initially respectfully submitted to be allowable on the basis of this dependency. Claim 10 includes limitations similar to claim 3, and thus the arguments set forth in favor of the allowability of claim 3 on its own merit apply with equal force in favor of claim 10.

Again, applicants wish to express their appreciation for the Examiner's allowance of claims 4-11 and 12. However, it is respectfully submitted that claim 1-3 and 5-10 should also be allowed. Reconsideration and allowance of these claims is respectfully solicited.

Respectfully submitted,

Paul J. Winters
Reg. No: 25,246
Attorney for Applicant(s)

I certify that this document is being deposited on April 14, 2007 with the U.S. Postal Service as first class mail under 37 C.F.R. §1.8 addressed to the Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450

Signature

Paul J. Winters
Typed or printed name